Listing of Claims:

Claims 1-27 (canceled)

Claim 28 (omitted in error due to improper numbering).

Claim 29-34 (canceled)

Claim 35 (new): A method for verifying the security of an electronic transaction between a vendor providing a purchased item or service and a purchaser from that vendor, said method comprising the steps of

the purchaser obtaining from the vendor transaction information identifying the transaction;

at the purchaser electronically performing a message authentication code function on the transaction information and purchaser identification information including a secret key of the purchaser's to obtain secure information regarding the transaction and the purchaser;

providing the purchaser identification information and the secure information to the vendor;

the vendor transmitting the vendor transaction information, the purchaser identification information, and the secure information to a verifier;

the verifier using the purchaser's secret key to perform the same message authentication code function on the purchaser identification information and the transaction information received from the vender to determine whether the result of the verifier message authentication code function is the same as the secure information provided to the verifier by the vendor; and

if the result is the same, verifying the security of the electronic transaction.

Claim 36 (new): The method of claim 35 wherein said vendor transaction information includes the purchase amount.

Claim 37 (new): The method of claim 36 wherein the secure information is obtained by the step of performing a message authentication code function on at least some of the transaction information and purchaser information including a secret key of the purchaser's and the secure information is provided to the vendor at least a part of a credit card number.

Claim 38 (new): The method of claim 35 further comprising the step of adding a counter value to the transition information prior to electronically performing the message authentication code function at the purchaser.

Claim 39 (new): An apparatus for verifying the security of an electronic transaction between a vendor providing a purchased item or service and a purchaser from that vendor, said apparatus comprising:

a first input at the user for receiving from the vendor transaction information identifying the transaction;

Appl. No. 09/765,751
Amdt. Dated January 9, 2004
Reply to Office action of November 7, 2003

APP 1277

a first processor at the purchaser configured to receive the transaction information, purchaser identification information, and a purchaser's secret key and electronically to perform a message authentication code function on the transaction information and the purchaser identification information using the secret key to obtain secure information regarding the transaction and the user;

a first output configured to output a result of the message authentication code function to the vendor;

a first input at a verifier for receiving from the vendor the vendor transaction information, the purchaser identification information , and the secure information;

a second processor at the verifier for using the purchaser's secret key to perform the same message authentication code function on the purchaser identification information and the transaction information received from the vender to determine whether the result of the verifier message authentication code function is the same as the secure information provided to the verifier by the vendor; and

a second output at the verifier for outputting a verification of the security of the electronic transaction if the result of the verifier message authentication code function is identical to the received secure information.

Claim 40 (new): The apparatus of claim 39 wherein said vendor transaction information includes the purchase price.

Claim 41 (new): The apparatus of claim 39 wherein said secure information includes at least a part of a credit card number.